

WHAT IS CLAIMED IS:

1           1.     A method in a computer system for maintaining and digitally signing  
2     a unique authoritative electronic record, the method comprising the steps of:  
3                 receiving an original electronic record in a repository;  
4                 generating at least some first receipt information, wherein the first  
5     receipt information includes information relating to the original electronic record;  
6                 prepending the first receipt information at a beginning portion of the  
7     original electronic record;  
8                 generating at least some first identifying information, wherein the  
9     first identifying information includes a provable representation of the first receipt  
10    information;  
11                appending the first identifying information at an end portion of the  
12    original electronic record;  
13                storing the original electronic record with the prepended first receipt  
14    information and the appended first identifying information in the repository as an  
15    authoritative electronic record;  
16                receiving a request to review and optionally sign the authoritative  
17    electronic record at a remote location;  
18                computing a partial message digest of a proper subset of the  
19    authoritative electronic record;  
20                computing a complement of the proper subset of the authoritative  
21    electronic record;  
22                transmitting the partial message digest of the authoritative electronic  
23    record to the remote location;  
24                transmitting the complement of the proper subset of the authoritative  
25    electronic record to the remote location;  
26                computing a message digest, at the remote location, using the partial  
27    message digest and the complement of the proper subset of the authoritative  
28    electronic record;  
29                displaying the complement of the proper subset of the authoritative  
30    electronic record at the remote location;  
31                allowing a digital signature to be computed at the remote location  
32    using the computed message digest and a private key;

33                   returning the digital signature to the repository;  
34                   receiving the digital signature in the repository;  
35                   generating at least some second receipt information, wherein the  
36 second receipt information includes information relating to the signed authoritative  
37 electronic record;  
38                   prepending the second receipt information at a beginning portion of  
39 the signed authoritative electronic record;  
40                   generating at least some second identifying information, wherein the  
41 second identifying information includes a provable representation of the receipt  
42 information;  
43                   appending the second identifying information at an end portion of the  
44 signed authoritative electronic record;  
45                   determining whether the digital signature information represents a  
46 valid digital signature; and  
47                   amending, if the digital signature information is determined to  
48 represent a valid digital signature, the authoritative electronic record in the  
49 repository to include the digital signature information, the prepended second receipt  
50 information, and the appended second identifying information from the signed  
51 authoritative electronic record.

1           2.       The method of claim 1, wherein the step of receiving an original  
2 electronic record further comprises the step of adding time-stamp information to the  
3 original electronic record, wherein the time-stamp information comprises the time  
4 and the date when the original electronic record is received in the repository.

1           3.       The method of claim 1, wherein the digital signature information is  
2 created with the use of the message digest and a private key.

1           4.       The method of claim 1, wherein the first receipt information includes  
2 at least some digital signature information that is generated using a private key of  
3 the repository.

1           5.       The method of claim 1, wherein the proper subset of the authoritative  
2 electronic record comprises information prepended to beginning portion of the  
3 authoritative electronic record.

1           6.       The method of claim 1, wherein the complement of the proper subset  
2 of the authoritative electronic record comprises the original electronic record and  
3 information appended to the end portion of the original electronic record.

1           7.     The method of claim 1, wherein the steps of transmitting the partial  
2     message digest of the authoritative electronic record and transmitting the  
3     complement of the proper subset of the authoritative electronic record to the remote  
4     location include transmitting the partial message digest and transmitting the  
5     complement of the proper subset of the authoritative electronic record to the remote  
6     location in a single transmission.

1           8.     The method of claim 1, wherein at least one software program  
2     associated with the repository is utilized at the remote location.

1           9.     The method of claim 1, wherein the partial message digest includes  
2     information necessary to compute the message digest at the remote location.

1           10.    The method of claim 1, wherein the step of prepending the second  
2     receipt information at a beginning portion of the signed authoritative electronic  
3     record includes replacing the first receipt information with the second receipt  
4     information.

1           11.    The method of claim 1, wherein the second receipt information  
2     includes at least some digital signature information that is generated using a private  
3     key of the repository.

1           12.    The method of claim 1, wherein the second identifying information is  
2     generated using at least some repository information.

1           13.    The method of claim 1, wherein the second identifying information is  
2     generated using at least some user information.

1           14.    The method of claim 1, wherein the second identifying information is  
2     generated using at least some remote location information.

1           15.    The method of claim 1, wherein the step of appending the second  
2     identifying information at an end portion of the signed authoritative electronic  
3     record includes amending the first identifying information to include the second  
4     identifying information.

1           16.    A method in a computer system for maintaining and digitally signing  
2     a unique authoritative electronic record, the method comprising the steps of:  
3     providing for the receipt of an original electronic record in a  
4     repository;  
5     providing for the generation of at least some first receipt information,  
6     wherein the first receipt information includes information relating to the original  
7     electronic record;

8 providing for the prepending of the first receipt information at a  
9 beginning portion of the original electronic record;  
10 providing for the generation of at least some first identifying  
11 information, wherein the first identifying information includes a provable  
12 representation of the first receipt information;  
13 providing for the appending of the first identifying information at an  
14 end portion of the original electronic record;  
15 providing for the storage of the original electronic record with the  
16 prepended first receipt information and the appended first identifying information in  
17 the repository as an authoritative electronic record;  
18 providing for the receipt of a request to review and optionally sign  
19 the authoritative electronic record at a remote location;  
20 providing for the computation of a partial message digest of a proper  
21 subset of the authoritative electronic record;  
22 providing for the computation of a complement of the proper subset  
23 of the authoritative electronic record;  
24 providing for the transmission of the partial message digest and the  
25 complement of the proper subset of the authoritative electronic record to the remote  
26 location;  
27 providing for the computation of a message digest, at the remote  
28 location, using the partial message digest and the complement of the proper subset  
29 of the authoritative electronic record;  
30 providing for the display of the complement of the proper subset of  
31 the authoritative electronic record at the remote location;  
32 providing for at least some digital signature information to be  
33 generated at the remote location using the computed message digest and a private  
34 key;  
35 providing for the receipt of the digital signature information in the  
36 repository;  
37 providing for the generation of at least some second receipt  
38 information, wherein the second receipt information includes information relating to  
39 the signed authoritative electronic record;  
40 providing for the prepending of the second receipt information at a  
41 beginning portion of the signed authoritative electronic record;

42 providing for the generation of at least some second identifying  
43 information, wherein the second identifying information includes a provable  
44 representation of the receipt information;  
45 providing for the appending of the second identifying information at  
46 an end portion of the signed authoritative electronic record;  
47 providing for the determination of whether the digital signature  
48 information represents a valid digital signature; and  
49 providing for the amending, if the digital signature information is  
50 determined to represent a valid digital signature, of the authoritative electronic  
51 record in the repository to include the digital signature information, the prepended  
52 second receipt information, and the appended second identifying information from  
53 the signed authoritative electronic record.

1 17. A method for creating an authoritative electronic record in a  
2 repository, the method comprising the steps of:  
3 receiving an original electronic record in a repository;  
4 generating at least some first receipt information, wherein the first  
5 receipt information includes information relating to the original electronic record;  
6 prepending the first receipt information at a beginning portion of the  
7 original electronic record;  
8 generating at least some first identifying information, wherein the  
9 first identifying information includes a provable representation of the first receipt  
10 information;  
11 appending the first identifying information at an end portion of the  
12 original electronic record; and  
13 storing the original electronic record with the prepended first receipt  
14 information and the appended first identifying information in the repository as an  
15 authoritative electronic record.

1 18. The method of claim 17, wherein the step of receiving an original  
2 electronic record further comprises the step of adding time-stamp information to the  
3 original electronic record, wherein the time-stamp information comprises the time  
4 and the date when the original electronic record is received in the repository.

1 19. The method of claim 17, wherein the digital signature information is  
2 created with the use of the message digest and a private key.

1           20.    The method of claim 17, wherein the first receipt information  
2 includes at least some digital signature information that is generated using a private  
3 key of the repository.

1           21.    A method for storing an original electronic record as an authoritative  
2 electronic record in a repository, the method comprising the steps of:

3                   transmitting an original electronic record to a repository;

4                   allowing at least some first receipt information to be generated,  
5 wherein the first receipt information includes information relating to the original  
6 electronic record;

7                   allowing the first receipt information to be prepended at a beginning  
8 portion of the original electronic record;

9                   allowing at least some first identifying information to be generated,  
10 wherein the first identifying information includes a provable representation of the  
11 first receipt information;

12                  allowing the first identifying information to be appended at an end  
13 portion of the original electronic record; and

14                  allowing the original electronic record to be stored with the  
15 prepended first receipt information and the appended first identifying information in  
16 the repository as an authoritative electronic record.

1           22.    A method for displaying a provable representation of an authoritative  
2 electronic record at a remote location, the method comprising the steps of:

3                   receiving a request to review and optionally sign an authoritative  
4 electronic record stored in a repository, at a remote location, wherein the  
5 authoritative electronic record includes at least some first receipt information  
6 prepended at a beginning portion of the authoritative electronic record, and at least  
7 some first identifying information, appended at an end portion of the original  
8 electronic record, wherein the first identifying information includes a provable  
9 representation of the first receipt information;

10                  computing a partial message digest of a proper subset of the  
11 authoritative electronic record;

12                  computing a complement of the proper subset of the authoritative  
13 electronic record;

14                  transmitting the partial message digest of the authoritative electronic  
15 record to the remote location;



receiving a complement of the proper subset of the authoritative  
electronic record from a repository;  
receiving a partial message digest of the authoritative electronic  
record from a repository;  
computing a message digest of the authoritative electronic record  
using the complement of the proper subset of the authoritative electronic record and  
the partial message digest of the authoritative electronic record;  
allowing a private key to be used to generate at least some digital  
signature information; and  
transmitting the digital signature information to the repository.

31. A method for including a valid digital signature in an authoritative  
electronic record stored in a repository, wherein the authoritative electronic record  
includes at least some first receipt information prepended at a beginning portion of  
the authoritative electronic record, and at least some first identifying information  
appended at an end portion of the authoritative electronic record, wherein the first  
identifying information includes a provable representation of the first receipt  
information, the method comprising the steps of:

receiving at least some digital signature information, wherein the  
digital signature information was generated using a private key and a message  
digest, wherein the message digest is computed using a partial message digest of the  
authoritative electronic record and a complement of a proper subset of the  
authoritative electronic record;

determining whether the digital signature information represents a  
valid digital signature; and

amending, if the digital signature information is determined to  
represent a valid digital signature, the authoritative electronic record to create a  
signed authoritative electronic record, wherein the signed authoritative electronic  
record comprises the authoritative electronic record and the digital signature  
information.

32. The method of claim 31, wherein the step of amending, if the digital  
signature information is determined to represent a valid digital signature, a signed  
authoritative electronic record includes the steps of:

prepending digital signature information comprising a digital  
signature to the beginning portion of the authoritative electronic record; and



6                appending digital signature information comprising a provable  
7       representation of the digital signature information to the end portion of the  
8       authoritative electronic record.

1                33.       The method of claim 31, wherein the step of amending, if the digital  
2       signature information is determined to represent a valid digital signature, a signed  
3       authoritative electronic record includes the steps of:

4                prepending at least some signature receipt information to the  
5       beginning portion of the authoritative electronic record, wherein the signature  
6       receipt information comprises a unique representation of the signed authoritative  
7       electronic record; and

8                appending at least some identifying information to the end portion of  
9       the authoritative electronic record, wherein the identifying information comprises a  
10       provable representation of the signature receipt.

1                34.       The method of claim 31, further including the steps of:

2                receiving a request, from a remote location, to review and optionally  
3       sign the signed authoritative electronic record, wherein the signed authoritative  
4       electronic record includes validated digital signature information;

5                computing a partial message digest of a proper subset of the signed  
6       authoritative electronic record;

7                computing a complement of the proper subset of the signed  
8       authoritative electronic record;

9                transmitting the partial message digest of the signed authoritative  
10       electronic record to the remote location;

11                transmitting the complement of the proper subset of the signed  
12       authoritative electronic record to the remote location;

13                allowing a message digest to be computed, at the remote location,  
14       using the partial message digest and the complement of the proper subset of the  
15       signed authoritative electronic record;

16                allowing the complement of the proper subset of the signed  
17       authoritative electronic record to be displayed at the remote location;

18                receiving at least some new digital signature information, wherein the  
19       new digital signature information was generated using a private key and the  
20       computed message digest;

determining whether the new digital signature information represents a valid digital signature; and  
amending, if the new digital signature information is determined to represent a valid digital signature, the signed authoritative electronic record to include the new digital signature information.

35. The method of claim 34, wherein the partial message digest includes information necessary to compute the message digest at the remote location.

36. A computer system for maintaining and updating a unique authoritative electronic record, the system comprising:  
means for receiving an original electronic record;  
means for generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record;

means for prepending the first receipt information at a beginning portion of the original electronic record;

means for generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information;

means for appending the first identifying information at an end portion of the original electronic record;

means for storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as an authoritative electronic record;

means for receiving a request to review and optionally sign the authoritative electronic record at a remote location;

means for computing a partial message digest of a proper subset of the authoritative electronic record;

means for computing a complement of the proper subset of the authoritative electronic record;

means for transmitting the partial message digest and the complement of the proper subset of the authoritative electronic record to the remote location;

means for computing a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record;

means for displaying the complement of the proper subset of the authoritative electronic record at the remote location;

means for allowing at least some digital signature information to be generated at the remote location, wherein the digital signature information is generated using the computed message digest and a private key;

means for receiving the digital signature information in the repository;

means for generating at least some second receipt information, wherein the second receipt information includes information relating to the signed authoritative electronic record;

means for prepending the second receipt information at a beginning portion of the signed authoritative electronic record;

means for generating at least some second identifying information, wherein the second identifying information includes a provable representation of the receipt information;

means for appending the second identifying information at an end portion of the signed authoritative electronic record;

means for determining whether the digital signature information represents a valid digital signature; and

means for amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record in the repository to include the digital signature information, the prepended second receipt information, and the appended second identifying information from the signed authoritative electronic record.

37. A system for creating an authoritative electronic record in a repository, the system comprising:

a software program that is capable of receiving an original electronic record;

a software program that is capable of generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record;

a software program that is capable of prepending the first receipt information at a beginning portion of the original electronic record;

a software program that is capable of generating at least some first

11 identifying information, wherein the first identifying information includes a  
12 provable representation of the first receipt information;  
13 a software program that is capable of appending the first identifying  
14 information at an end portion of the original electronic record; and  
15 a software program that is capable of storing the original electronic  
16 record with the prepended first receipt information and the appended first identifying  
17 information in the repository as an authoritative electronic record.

1 38. A system for obtaining a digital signature on an authoritative  
2 electronic record stored in a repository, the system comprising:

3 a software program that is capable of receiving a request to review  
4 and optionally sign an authoritative electronic record, stored in a repository, at a  
5 remote location, wherein the authoritative electronic record includes at least some  
6 first receipt information prepended at a beginning portion of the authoritative  
7 electronic record, and at least some first identifying information, appended at an end  
8 portion of the authoritative electronic record, wherein the first identifying  
9 information includes a provable representation of the first receipt information;

10 a software program that is capable of computing a partial message  
11 digest of a proper subset of the authoritative electronic record;

12 a software program that is capable of computing a complement of the  
13 proper subset of the authoritative electronic record;

14 a software program that is capable of controlling the transmission of  
15 the complement of the proper subset of the authoritative electronic record, the partial  
16 message digest and the complement of the proper subset of the authoritative  
17 electronic record to the remote location;

18 a software program that is capable of allowing a message digest to be  
19 computed, at the remote location, using the partial message digest and the  
20 complement of the proper subset of the authoritative electronic record;

21 a software program that is capable of allowing the complement of the  
22 proper subset of the authoritative electronic record to be displayed at the remote  
23 location; and

24 a software program that is capable of allowing at least some digital  
25 signature information to be generated using the computed message digest and a  
26 private key.

39. A system for including a valid digital signature in an authoritative electronic record stored in a repository, wherein the authoritative electronic record includes at least some first receipt information prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information appended at an end portion of the authoritative electronic record, wherein the first identifying information includes a provable representation of the first receipt information, the system comprising:

a software program that is capable of receiving at least some digital signature information produced using a computed message digest and a private key, wherein the computed message digest is generated using a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record;

a software program that is capable of determining whether the digital signature information represents a valid digital signature;

a software program that is capable of amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record includes the authoritative electronic record and the digital signature information; and

a software program that is capable of storing the signed authoritative electronic record in the repository as the authoritative electronic record.

40. A computer program product for obtaining a digital signature on a single authoritative copy of an original electronic record comprising:

a computer usable medium and computer readable code embodied on the computer usable medium for obtaining a digital signature on a single authoritative copy of an original electronic record, the computer readable code comprising:

computer readable program code devices configured to cause the computer to effect the storing of an original electronic record as an authoritative electronic record in a repository;

computer readable program code devices configured to cause the computer to effect the transmission of a provable representation of an authoritative electronic record from a repository to a remote location, wherein the provable representation of the authoritative electronic record includes a partial message digest

14 of the authoritative electronic record and a complement of a proper subset of the  
15 authoritative electronic record;

16 computer readable program code devices configured to cause the  
17 computer to effect the generation of at least some digital signature information,  
18 wherein the digital signature information is produced using a computed message  
19 digest and a private key, wherein the computed message digest is generated using  
20 the partial message digest of the authoritative electronic record and the complement  
21 of a proper subset of the authoritative electronic record;

22 computer readable program code devices configured to cause the  
23 computer to effect the transmission of the digital signature information from the  
24 remote location to the repository and the receipt of the digital signature information  
25 in the repository;

26 computer readable program code devices configured to cause the  
27 computer to effect the amending, if the received digital signature information is  
28 determined to be valid, of the authoritative electronic record in the repository to  
29 include at least some of the received digital signature information.